Examining Employee Social Media Deviance: A Psychological Contract Breach Perspective

Bowen Guan
The University of Sydney
bowen.guan@sydney.edu.au

Carol Hsu
The University of Sydney
carol.hsu@sydney.edu.au

Feng Xu
Mississippi State University
fx25@msstate.edu

Abstract

With the prevalence of social media, employees' deviant behaviors on social media can go viral and result in unpredictable negative outcomes beyond the workplace. This paper investigates the relationship between abusive supervision and employee social media deviance from the theoretical perspective of psychological contract breach (PCB), and examines the moderating role of social media controls. Building on prior studies of abusive supervision and employee workplace deviance, this paper argues that abusive supervision plays a crucial motivational role in triggering employee social media deviance. Our results demonstrate that employees who experience abusive supervision are more likely to perceive PCB, and thus engage in social media deviance. User awareness of social media policy and informal sanctions can weaken the positive relationship between employee perceived PCB and social media deviance.

1. Introduction

Social media has many transformative impacts of information technology on business both within and outside organizations by changing the way we communicate and work [1]. It allows individuals to interact with others and express themselves without physical boundaries restriction, and consequently, the issue of employee social media usage has increasingly raised many concerns for both researchers and practitioners [2]. The boundaries of employees' workplace deviance can be extended by social media from on-duty deviance to off-duty deviance, as social media might be used inappropriately by insider employees to cause harm to organizations anytime and anywhere. For example, employees might use social media for non-work-related purpose during office hours, leading to the decline of productivity [2]; sharing offensive or negative comments about their organizations, supervisors or coworkers that might hurt others' physical or psychological well-being and sabotage the corporate brand [3]; disclosing confidential information of corporations, which might result in unpredictable losses for organizations [4]. Therefore, there is a call that "these negative outcomes, often described as deviant behaviors, are a cautionary tale in the widespread proliferation of social media [5, p. 864]".

We define employee social media deviance as socially and/or organizationally deviant behaviors that focus on social media communications and threatens the well-being of the organization and/or its members. In general, previous studies mainly focused on general users' deviant behaviors on social media, rather than employees. In fact, researchers do not have a good theoretical understanding of the contextual factors that play a role of prevention and control in employee social media deviance [5]. Given the importance of social media governance for organizational IT issues, more research efforts need to be devoted to the causes and preventions of employee social media deviance.

In this research, we claim that abusive supervision plays a crucial role in influencing employee social media deviance. There are considerable evidences that abusive supervision, which is defined as "employees' perceptions of the extent to which supervisors engage in the sustained display of hostile verbal and nonverbal behaviors, excluding physical contact [6, p. 178]", can cause a broad range of destructive outcomes on subordinates, including lower job satisfaction, lower organizational commitment, and employee workplace deviance [6, 7, 8]. Particularly, Hornstein [9] found that subordinates often tend to seek "payback" as the response to their leaders' abusive supervision by using IT-related methods, such as posting their boss's email or photos on websites, or sabotaging the company's payroll program. Considering that social media could be easily accessed within and outside the workplace, in respond to abusive supervision, it is more likely for

URI: https://hdl.handle.net/10125/79710
978-0-9981331-5-7

employees to use social media as a popular "payback" method to take revenge against a particular person or the entire organization. On the other hand, as highlighted in IS research, many IT-related deviant behaviors have been highly associated with employees' perceptions of unfair supervisory treatment (i.e., perceived organizational injustice), such as cyberloafing [10, 11], computer abuse [12, 13], and information security policy noncompliance [14]. Therefore, based on these evidences, we consider that abusive supervision might be a motivational factor in employees' engagement in social media deviance.

Thus, our research objective is to empirically investigate the relationship between abusive supervision and employee social media deviance. To further understand motivational factors, we draw upon psychological contract breach (PCB) theory, which has been found to be motivated by employees' perceptions of unfair interactions with their organizations [15] and have a positive effect on employee workplace deviance [16]. We believe that, employees who perceive PCB which is triggered by abusive supervision are more likely to engage in social media deviance. Furthermore, to enrich our insight, we consider several social media controls as the countermeasures which might play a deterrent role in employee social media deviance. Similar to prior IS security studies, user awareness of formal and informal sanctions against security breaches can effectively mitigate employees' IT-related deviant behaviors by increasing their perceptions of certainty and severity of sanctions [17, 18]. Align with this notion, we consider two formal controls (i.e., social media policy, Internet monitoring) and one informal control (i.e., informal sanctions) might have deterrent impact on employee social media deviance. We examine their moderating roles in the relationship between employees' perceived PCB and social media deviance. Overall, we believe that, user awareness of social media policy, Internet monitoring and informal sanctions, would weaken the positive effect of employees' perceived PCB on employee social media deviance.

This paper is organized as follows. The next section reviews existing literature on employee social-media-deviance-related behaviors. Then we discuss our theoretical hypotheses and present the research model. This is followed by the research methodology and empirical results of this study. Next, we discuss the empirical results and conclude the paper with the theoretical and practical implications of this research.

2. Literature review

We conduct the literature review within the scope of relevant deviant behaviors committed by employees on social media. The most common social media deviance is non-work-related social media usage in the workplace [2, 19]. This phenomenon has been generalized in IS research as cyberloafing, which refers to "not necessarily have malicious intents to harm the security or general business operations of the organization [20, p.205]". Consistent with this notion, employees using social media for non-work-related purposes during office hours can be considered as a non-malicious violation in the workplace, just for taking a mental break from work [2], and has been demonstrated by Andreassen et al. [2] and Lu et al. [19], that it would be detrimental to employees' job performance and productivity. In recent years, researchers have paid increasing attention to the motives for cyberloafing, including habit, affect, attitude [21], norms [22], social factors, formal controls [23], personality traits [24], and emotional intelligence [25]. However, these studies yielded mixed results on the direct motivational effect of these antecedents. Vance et al. [23] suggested that formal controls can effectively reduce cyberloafing by increasing employees' perceptions of accountability. Khansa et al. [26] identified neutralization, perceived risk as significant antecedents of employee cyberloafing, and showed that some antecedents were not significant after the announcement of formal controls. They called on that further research should extend additional predictors of cyberloafing and investigate the interactional effects among them. Thus, our perspective on employee social media deviance is rooted in this argument, trying to empirically examine its potential motives.

In addition, other previous studies focused on employees' inappropriate social media usage behaviors, which include aggressive, intentional acts through written-verbal (i.e., abusive emails) or visual ways (i.e., posting embarrassing videos) [27]. Such social media deviance is often committed with a malicious intention to do harm to others, like cyberbullying. Evidences from previous studies showed that cyberbullying in the workplace can harm employees' psychological and physical well-being, including greater mental stress, lower job satisfaction and commitment, and higher turnover intention [27, 28]. Researchers have recognized that cyberbullying has spread from purely social contexts to business contexts and social media plays an important role in spreading cyberbullying with a rapid, broad scale that it is almost unstoppable [5]. Nonetheless, to the best of our knowledge, a key shortcoming of these lens of studies is the lack of empirical studies providing theoretical insights on the motivations of such social media deviance using quantitative method. Nocentini et al. [28] identified some motivating factors that influence cyberbullying, including the sense of anonymity, lower threshold, and

the lack of rules, control and awareness. Their main research objective was to define cyberbullying with the most suitable item by examining four typologies of behaviors which all represent the cyberbullying construct. This research did not provide empirical evidence linking cyberbullying with its motivational factors.

Overall, we find the research value of extending the predictors of employee social media deviance with a theoretical foundation. To address this research gap, we aim to theoretically investigate the motives of social media deviance from the perspective of abusive supervision, as we briefly note in the introduction. We then theorize and empirically test the motivational role of abusive supervision on employee social media deviance in the next section.

3. Theoretical background and hypothesis development

3.1 Abusive supervision

Widely being discussed in organizational behavioral studies, abusive supervision, as an unfair supervisory treatment, has been reported that it is negatively associated with employees' job satisfaction, job performance, organizational commitment, perceptions of organizational injustice, and psychological distress [6,7,8], and could also result in employee workplace deviance to retaliate directly against their abusive supervisors [7,8]. These findings support for IS scholars regarding abusive supervision as an important predictor of employees' IT-related deviant behaviors. In fact, drawing upon organizational justice theory, previous IS studies have demonstrated that employees' perceptions of injustice treatment from organizations play a crucial role in employee security breaches. For instance, Lim [10] found that employees were more likely to rationalize cyberloafing when they perceived injustice (i.e., being unjustly treated or underpaid) from organizations. Willison et al. [13] examined employees' perceived organizational injustice as the motive of computer abuse. And Guan & Hsu [14] demonstrated that abusive supervision can play the motivational role in employees' information security policy noncompliance intention by raising their perceptions of interactional injustice. Conceptualizing employee social media deviance as a kind of IT-related deviant behavior in the IS context, these findings provide us sufficient evidence to consider abusive supervision as a potential motive of employee social media deviance. In particular, employees may consider that off-duty conduct on social media outside the workplace is unrelated to supervisors' responsibility with regard to workplace conduct [29], which increases the possibilities of using social media to exact revenge in a digital environment. Fewer workplace barriers of social media exacerbate employees' engagement in social media deviance when they perceive abusive supervision from organizations. Therefore, we argue that abusive supervision might have a critical motivational effect on employee social media deviance.

3.2 Psychological Contract Breach

Psychological contract breach (PCB) is defined as "the cognition that one's organization has failed to meet one or more obligations within one's psychological contract in a manner commensurate with one's contributions [15, p.230]. Organizations unable or unwilling to fulfill promised obligations (i.e., reneging), and the discrepancy between what employee experienced and what they had expected (i.e., incongruence), are the two basic factors that contribute to employee's perception of PCB [15, 30]. Previous research suggested that PCB would be heavily influenced by employees' perceived interactional fairness or beliefs about the interpersonal treatment they experienced [15]. For example, Robinson & Morrison [30] confirmed that employees are more likely to perceive PCB when they were treated with little consideration or respect. Roninson [31] indicated that employees may perceive PCB as a form of distributive inequity or imbalance in the employees-organizations relationship.

In particular, attention has been paid to the link between PCB and abusive supervision. There is no doubt that abusive supervision represents an unfair and negative situation and much attention has been paid to the link between PCB and abusive supervision. Ahmed & Muchiri [32] presented a conceptual model in which they proposed that PCB mediated the relationship between abusive supervision and employees' organizational citizenship behavior and turnover intentions. They highlight that employees' perceptions of PCB can be created when they perceive abusive supervision, which involves high imbalance in the relationship within a psychological contract [32]. Thus, we argue that abusive supervision could increase employees' perception of organization failing to adequately fulfill the psychological contract. As such, we hypothesize the following:

Hypothesis 1: Abusive supervision is positively associated with employee perceived psychological contract breach.

Furthermore, many focuses have also been placed on the relationship between PCB and employee workplace deviance [33, 34]. Chiu & Peng [33] suggested that PCB could elicit employees' negative

cognitive evaluations and negative emotional reactions to organization, which in turn trigger negative deviant behaviors, such as retaliation and aggression. Within IS literature, researchers drew upon the psychological contract perspective to examine employees' IT-related deviant behaviors. For example, Han et al. [35] reported that employee perceived psychological contract fulfillment had a mediating effect on the relationship between perceived cost and information security policy compliance intention. Lin et al. [36] suggested that user perceived PCB could increase user resistance to an IS implementation directly and indirectly via feeling of violation. Again, these findings imply that PCB would be a significant predictor of various employees' IT-related deviant behaviors. In our context, we contend that employee social media deviance, with the characteristics of both on-duty and off-duty, could be regarded as an IT-related deviant behavior to express their retaliation and aggression, and is more likely to occur when employees perceive PCB which is caused by abusive supervision they suffered. Thus, we propose the following hypothesis.

Hypothesis 2: Employee perceived psychological contract breach is positively associated with employee social media deviance.

3.3 Moderating factors: user awareness of social media policy, Internet monitoring, and informal sanctions

In this section, we discuss three formal and informal social media controls and explore their moderating roles on mitigating employee social media deviance. Consistent with the importance of information security awareness in minimizing the misuse of information technologies highlighted in prior IS literature [17, 37], we focus on user awareness of social media policy, Internet monitoring, and informal sanctions as interventions and examine their moderating effects between employee perceived PCB and employee social media deviance. Previous studies have suggested that deterrent controls can effectively reduce employees' negative workplace behaviors stemming from motives and thus negatively moderates the relationship between motives and negative behavior [13, 38].

Social media policy. Much attention has been paid to developing social media policy to regulate employees' participation in social media, due to the potential risks of employee social media deviance. In general, social media policy consists of a series of formal guidelines, which regulate employees' obligations for the proper use of social media both within and outside the workplace, involving prohibitions on harassment, discrimination, posting offensive comment, and disclosure of confidential information, as well as sanctions for inappropriate social media usage [39, 40]. It has been widely recognized that social media policy would be an important countermeasure for organizations to prevent employees from engaging in illegal or unethical behaviors on social media [39, 40]. Specially, Thornthwaite [40] indicated that organizational social media policy could provide significant protections to limit employees' off-duty online activities about working lives, potentially regulating "not only collective dissent but also the expression of individual opinion and voice (p.333)".

In the IS literature, previous studies have largely emphasized the implementation of information security policy (ISP) as a deterrent formal control in minimizing employees' computer misuse and IS security breaches [17, 37, 41]. For example, drawing upon the deterrence approach, D'Arcy et al. [17] considered security policy had underlying deterrent mechanism and could be internal measures to punish employees IS misuse behavior. They examined the direct and indirect effects of security policy on employees IS misuse intention, and suggested that user awareness of security policy could increase the perceived severity of sanctions, which in turn significantly deterred employees IS misuse [17]. Lowry et al. [42] showed that the explanation adequacy of security policy increased trust, which significantly reduced reactive computer abuse. Thus, given the effectiveness of ISP in deterring employee security breaches, in our context, we consider that social media policy may have the same deterrent impact on employee social media deviance. We argue that when user awareness of social media policy is high, employees would be less likely to engage in social media deviance even though they perceived psychological contract breach. Thus, we hypothesize that:

Hypothesis 3: User awareness of social media policy moderates the effect of employee perceived PCB on social media deviance, such that the effect is weaker when the awareness of social media policy is high.

Internet monitoring. As an active security measure to regulate employees' online activities, Internet monitoring has been widely discussed in IS studies about its effectiveness of regulating employees' IS security breaches. D'Arcy et al. [17] suggested that monitoring practices enable the detection of serious and deliberate IS misuse incidents by increasing employees' perceived certainty and severity of sanctions as they would interpret the devotion of resources to monitoring as a warning of severe punishment for violations. Ugrin et al. [43] found that employees' awareness of detection and monitoring systems significantly deterred employees' intention to

cyberslacking by increasing their perceptions of sanctions. Henle et al. [11] indicated that the periodic monitoring significantly decreased employees' cyberloafing frequency.

Meanwhile, Internet monitoring can also play a crucial role in social media activities surveillance. In recent years, social media monitoring technologies, like deep content inspection-based security solutions, intrusion detection and prevention systems, can track employees' use of social media, monitor the content creation and defend against wide attacks [39]. Due to the deterrence effect of Internet monitoring on employees' security breaches, the effects of motives, such as perceived workplace stress and injustice, on employees' workplace deviance were weakened [10, 44]. Thus, we consider that when user awareness of social media policy and internet monitoring is high, employees who perceived PCB would be less likely to engage in social media deviance. We hypothesize that:

Hypothesis 4: User awareness of Internet monitoring moderates the effect of employee perceived PCB on social media deviance, such that the effect is weaker when the awareness of Internet monitoring is high.

Informal sanctions. Distinct with social media policy and Internet monitoring, informal sanctions, as an informal control, refers to individuals' certainty and severity perception of the loss of respect and disapproval from peers or friends [45], and it is regarded as another deterrent countermeasure with "non-legal costs" [46]. Hollinger & Clark [47] showed that informal sanctions was positively related to employee compliance behavior. In IS research, Siponen & Vance [18] indicated that informal sanctions had significant negative effect on employees' intention to violate ISPs without the neutralization construct. Johnston et al. [48] suggested that perceived informal sanctions was significant in their roles as direct determinants of compliance intention. Consistent with these important evidences, in our context, we believe that if an employee consider that important supervisors or coworkers may disapprove of their non-work-related social media usage in the workplace, and condemn their inappropriate postings against organizations, they are more likely to reduce their social media deviance. Thus, we argue that employees who perceived PCB due to their abusive supervisor are less likely to engage in social media deviance if they are highly aware of informal sanctions. Therefore, we hypothesize the following:

Hypothesis 5: User awareness of informal sanctions moderates the effect of employee perceived PCB on social media deviance, such that the effect is weaker when the awareness of informal sanctions is high.

Overall, we establish our research model which illustrates the relationships among abusive supervision, perceived PCB and social media deviance, as well as the moderating role of user awareness of social media policy, internet monitoring, and informal sanctions. All the proposed hypotheses are shown in Figure 1.

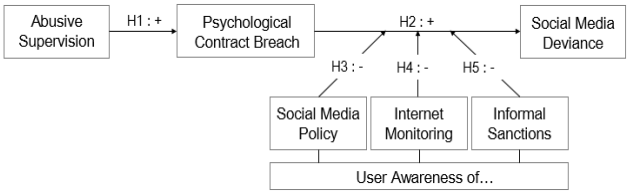


Figure 1. Research Model

4. Research methodology

To test the relationships implied by the research hypotheses, this research used a survey instrument for data collection. The measurement of abusive supervision was adopted from Tepper [6]. Employees' perceived of PCB was measured with the instruments developed by Robinson & Morrison [29]. Measurements of user awareness of social media policy, internet monitoring, and informal sanctions were adapted from D'Arcy et al. [17], Posey et al. [12] and Siponen & Vance [18]. In particular, we developed the measurement of employee social media deviance based on previous empirical social media studies [10, 49]. Respondents were asked to respond to statements, such as "I have posted negative or inappropriate content about my organization on social media", "I have browsed social network sites for non-work-related activities during working hours". All the items were measured using a five-point Likert agreement scale (anchored from 1="Strongly Disagree" to 5="Strongly Agree").

We refined, restructured, and deleted some items after the pretest. To further determine instrumental reliability and validity, a pilot test was performed through an online questionnaire issued on the Amazon Mechanical Turk (MTurk), targeting employees who were over 18 years old, working full-time, and made aware of their organizations' social media policy. Following with previous studies, we also controlled age, gender, education, income, organizational tenure, tenure with supervisor, organizational size (number of employees) and social media usage (hours per day).

Our survey was designed with two stages, which were conducted before (Time 1) and after (Time 2) at least one-month interval, in line with the method approached by previous studies on abusive supervision [8], as it allowed us to investigate the time-separated effects of abusive supervision [8] and to minimize the effect of common method bias. Participants were paid for their participation in both Time 1 and Time 2. In Time 1, we measured abusive supervision user

awareness of social media policy, Internet monitoring, informal sanctions as well as demographic information and control variables. In Time 2, participants were asked to answer the questions about their perceptions of PCB and social media deviance. A total of 337 participants who completed the Time 1 survey met our requirements, and finally, data provided by 283 respondents who completed both Time 1 and Time 2 could be used for further analysis. The demographic information of 283 respondents showed that 57% of our participants were male, 85.9% respondents were between 25 and 44 years of age, more than half of the respondents had an undergraduate degree, the annual income of 66.8% respondents was below $50,000, and 90.1% respondents spend more than 45% of 24 hours per day on using social media.

Results of the t-test of the differences of participants' perceived abusive supervision between the usable responses in Time 1 and Time 2 suggested that there were no concerns on non-response bias in this study.

5. Data analysis and results

5.1 Measurement model

We used AMOS version 22.0 to estimate and validate our measurement model. As shown in Table 1, all the Cronbach'α were greater than the general criteria of 0.70 [50], thus, our instruments had good internal consistency reliability. The results of factor loadings were above 0.60 [50], supporting good individual item reliability. The convergent validity was assessed by composite reliability (CR) and average variance extracted (AVE).

Table 1. Results of Reliability and Validity

Constructs	Items	CR	AVE	Loading	Cronbach'α
Abusive Supervision	AS1	0.939	0.732	0.909	0.946
	AS2			0.903	
	AS3			0.993	
	AS4			0.859	
	AS5			0.847	
	AS6			0.766	
Psychological Contract Breach	PCB1	0.932	0.784	0.953	0.921
	PCB2			0.743	
	PCB3			0.828	
	PCB4			0.934	
Social Media Deviance	SMD1	0.814	0.597	0.714	0.802
	SMD2			0.725	
	SMD3			0.779	
	SMD4			0.884	
Social Media Policy	SMP1	0.806	0.695	0.998	0.794
	SMP2			0.756	
Internet Monitoring	IntM1	0.926	0.717	0.833	0.939
	IntM2			0.979	
	IntM3			0.862	
	IntM4			0.794	
	IntM5			0.799	
Informal Sanctions	InfS1	0.877	0.648	0.718	0.878
	InfS2			0.776	
	InfS3			0.888	
	InfS4			0.897	

Table 2 shows that the CR values ranged from 0.806 to 0.939, which exceeded the threshold value of 0.70 [50], and the AVEs were all above the acceptable value of 0.50 [51] with a range from 0.597 to 0.784, suggesting the adequate convergent validity. The discriminant validity was assessed by checking the square root of the AVE [51]. As shown in Table 2, the square root of AVE for each construct was higher than the correlations between it and all other constructs, indicating good discriminant validity. Overall, these results showed that our measurement model had sound reliability and validity. Furthermore, as summarized in Table 3, our measurement model had an acceptable model fit.

Table 2. Correlations between Constructs

Construct	AS	PCB	SMD	SMP	IntM	InfS
AS	**0.856**					
PCB	0.593	**0.885**				
SMD	0.207	0.264	**0.773**			
SMP	0.053	0.092	-0.119	**0.834**		
IntM	0.176	0.169	0.099	0.455	**0.847**	
InfS	-0.062	-0.152	-0.182	-0.036	0.058	**0.805**

Table 3. Goodness of Fit

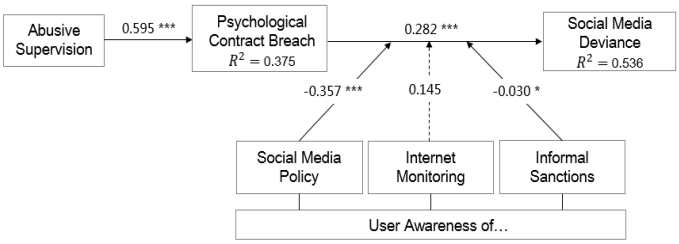
Fit Indices	χ^2 /df	GFI	AGFI	NFI
Observed Value	1.540	0.896	0.837	0.854
Desired Value	1-5	>0.85	>0.80	>0.80
Fit Indices	**TLI**	**CFI**	**RMR**	**RMSEA**
Observed Value	0.895	0.909	0.047	0.079
Desired Value	>0.80	>0.90	<0.10	<0.10

5.2 Structural model

In structural model testing performed on AMOS, all the path coefficients were significant with a p-value of less than 0.05, except the moderating path of user awareness of internet monitoring. This research model explained a significant portion of variance in social media deviance (R^2=0.536).

As shown in Figure 2, abusive supervision had a positive relationship with employee perceived PCB (H1: β=0.595, P<0.001), H1 was supported. PCB was found to be positively related to employee social media deviance (H2: β=0.282, P<0.01), supported H2. Two-way interaction items were created to analyze the moderating effect using the matched-pair strategy [52] and the double mean-centering method [53]. Results showed that user awareness of social media policy and informal sanctions significantly weaken the positive relationship between PCB and social media deviance (H3: β=-0.357, P<0.001; H5: β=-0.030, P<0.05), thus, H3 and H5 were supported. However, user awareness of internet monitoring was found to have a positive

moderating effect (H4: β=0.145, P>0.05), suggesting H4 was not supported.



Note: The unbroken lines indicate supported hypotheses, and the dotted lines indicate unsupported hypotheses. *p < 0.05; **p < 0.01; ***p < 0.001.

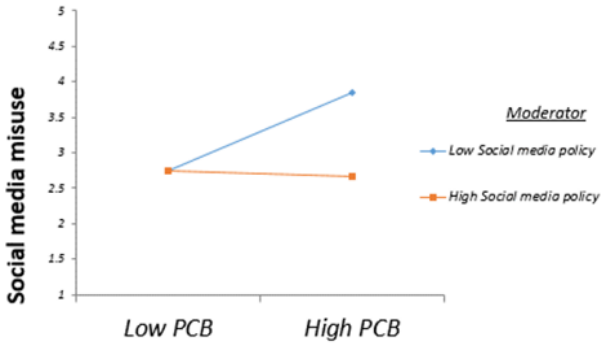
Figure 2. Results of Model Testing

In addition, a bootstrapping method with 5,000 bootstrap samples and a significance level of 0.05 were used to test the mediation effect of PCB. Following the procedures proposed by MacKinnon et al. [54] and Zhao et al. [55], we computed the bootstrapping results of an indirect effect by multiplying the results of certain direct effects. The results in Table 4 indicated that PCB statistically mediated the relationship between abusive supervision and employee social media deviance.

Table 4. Test for Mediation

Direct effect	Indirect effect	Confidence Interval		p-value
		Low	High	
0.094	0.200	0.086	0.101	0.035

To further examine the moderating effects, we conducted a simple slope analysis suggested by Dawson [56] to interrupt the significance of interaction items. As shown in Figure 3, for low social media policy with a high PCB, the level of social media deviance tended to be higher (i.e., the slope was steeper), suggesting that social media policy dampened the positive relationship between PCB and social media deviance. Similar pattern was seen in informal sanctions, although its slope changed slightly. However, the slope was steeper when Internet monitoring was higher, indicating that the positive effect of PCB on social media deviance was strengthened, thus, Internet monitoring played a positive moderating effect.



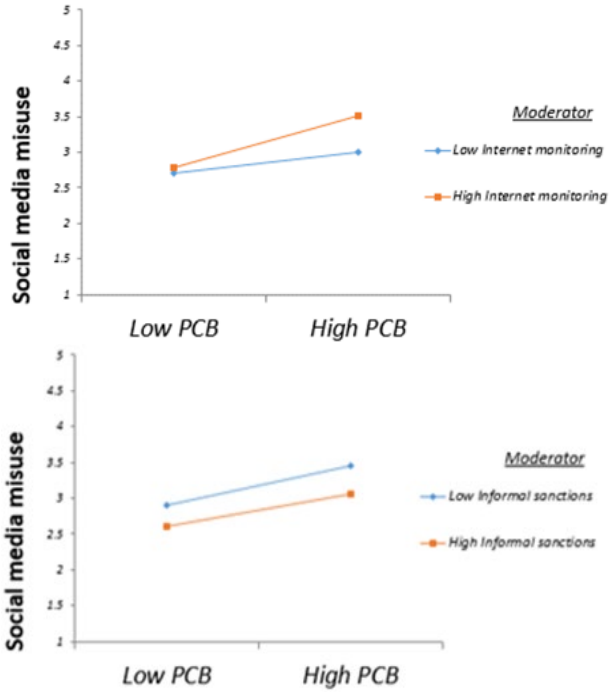


Figure 3. Results of Moderating Effects

6. Discussion and conclusions

This study has examined the relationship between abusive supervision and employee social media deviance from psychological contract breach perspective. Our findings have demonstrated that, when employees had suffered abusive supervision could perceive psychological contract breach, and their likelihood of social media deviance would be higher. Furthermore, our results indicated that user awareness of social media policy and informal sanctions have a significant and negative moderating effect on influencing the positive relationships between PCB and employee social media deviance, while Internet monitoring did not work. In fact, as Bies and Moag [57] concluded, Internet monitoring can be counterproductive for organizations that do not take into account the strong desire of their employees to be treated in a dignity and justice manner. In our context, when employees experienced abusive supervision, Internet monitoring might not be enough to deter their social media deviant behavior, exactly because social media provides an essential access for employees to express their voice when they are treated unfairly by their supervisors [2]. Furthermore, Posey et al. [12] found that, Internet monitoring might increase employees' computer abuse as it would "be perceived by employees as an invasion of privacy (p. 38)". This seems to provide another perspective to understand why user awareness of Internet monitoring might not

be an effective intervention on employee social media deviance.

We believe our research findings offer important theoretical contributions to social media research. First, the focus on employee social media deviance has been predominantly centered on a variety of inappropriate social media usage behaviors. Among these studies, the detrimental consequences of social media deviance have drawn much attention. However, to the best of our knowledge, a limited number of studies have examined the motivations of employee social media deviance. This research drew on abusive supervision and examines its motivational impact on employee social media deviance from the theoretical perspective of PCB. We believe further studies may be conducted to analyze employee social media deviance and other motivational factors. Second, based on the deterrence theory in IS studies, we explored the moderating role of formal and informal controls in deterring employee social media deviance. This responds to Willison et al. [13] recent call that examining the moderating effect of sanctions contributes to the relative sparse discussion of deterrence theory in forming employee deviant behaviors. Our findings first bring research attention to investigating the role of moderating factors in mitigating social media deviance, which provides a new insight to the discussion of employees' social media usage in organizations.

In addition, this research also has some implications for practice. First, our findings provide practical guidance for organization managers to better regulate employee social media usage within and outside the workplace. Our work demonstrates that abusive supervision is a unique contribution to employee social media deviance, and thus, attention should be paid to avoiding abusive supervision. Second, implementing deterrent countermeasures can be effective in dampening employees' intentions of social media deviance, like formal social media policy. And some informal sanctions, like shame, criticism, and disapproval, can also play a crucial role in enabling employees' behaviors to conform to the social norms of the society.

However, some research limitations exist. First, we used a self-reported method to collect data—a shortcoming has been reported that employees might respond dishonestly about deviant behaviors due to their worries about the retaliation by supervisors. Although we reduced the risk of social desirability bias as much as possible by adopting an anonymous approach, the measurement of actual deviant behavior might provide more reliable results. Second, the dynamic of employees' perceptions of abusive supervision can differ within a long period of time. Further research may conduct a longitudinal study to examine employees' perceptions of abusive supervision over time and provide more insights in different contexts. Third, future research might explore the motivational role of abusive supervision on different types of employee social media deviance, such as browsing social media for personal purposes and posting harmful messages about the company. The investigation of different types of deviance might enrich our understanding of employees' motives for performing social media behaviors.

7. References

[1] S. Aral, C. Dellarocas, and D. Godes, "Introduction to the special issue – social media and business transformation: a framework for research," Information Systems Research, 24(1), 2013, pp. 3-13

[2] C. S. Andreassen, T. Torsheim, and S. Pallesen, "Use of online social network sites for personal purposes at work: does it impair Self-Reported Performance?" Comprehensive Psychology, 3(1), 2014, Article 18.

[3] R.N. Landers, and R.C. Callan, "Validation of the beneficial and harmful work-related social media behavioral taxonomies: development of the work-related social media questionnaire," Social Science Computer Review, 32 (5), 2014, pp. 628-646.

[4] Forbes Agency Council, "The modern workplace: tips for creating an employee social media policy," https://www.forbes.com/sites/forbesagencycouncil/2020/04/17/, 2020 (accessed 17 April 2020).

[5] P. B. Lowry, G. D. Moody, and S. Chatterjee, "Using IT design to prevent cyberbullying," Journal of Management Information Systems, 34(3), 2017, pp. 863-901.

[6] B. J. Tepper, "Consequences of abusive supervision," Academy of Management Journal, 43(2), 2000, pp. 178-190.

[7] M. S. Mitchell and M. L. Ambrose, "Abusive supervision and workplace deviance and the moderating effects of negative reciprocity beliefs," Journal of Applied Psychology, 92(4), 2007, pp. 1159-1168.

[8] S. Thau and M. Mitchell, "Self-gain or self-regulation impairment? Tests of competing explanations of the supervisor abuse and employee deviance relationship through perceptions of distributive justice," Journal of Applied Psychology, 95(6), 2010, pp. 1009-1031.

[9] H. A. Hornstein, "Boss abuse and subordinate payback," Journal of Applied Behavioral Science, 52(2), 2016, 231-239.

[10] V. Lim, "The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice," Journal of Organizational Behavior, 23(5), 2002, pp. 675–694.

[11] C. A. Henle, G. Kohut and R. Booth, "Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyberloafing: an empirical test of justice theory," Computers in Human Behavior, 25(4), 2009, pp. 902-910.
[12] C. Posey, R. J. Bennett, T. L. Roberts and P. B. Lowry, "When computer monitoring backfires: invasion of privacy and organizational injustice as precursors to computer abuse," Journal of Information System Security, 7(1), 2011, pp. 24-47.
[13] R. Willison, M. Warkentin, and A. C. Johnston, "Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives," Information Systems Journal, 28(2), 2018, pp. 266–293.
[14] B. W. Guan and C. Hsu, "The role of abusive supervision and interactional justice in employee information security policy noncompliance intention," Proceedings of the 22nd Pacific Asia Conference on Information Systems (PACIS), 2018, 33.
[15] E. W. Morrison and S. L. Robinson, "When employees feel betrayed: a model of how psychological contract violation develops," Academy of Management Review, 22(1), 1997. pp. 226-256.
[16] P. Bordia, S. L. D. Restubog, and R. L. Tang, "When employees strike back: investigating mediating mechanisms between psychological contract breach and workplace deviance," Journal of Applied Psychology, 93(5), 2008, pp. 1104-1117.
[17] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," Information Systems Research, 20(1), 2009, pp. 79-98.
[18] M. Siponen and A. Vance, "Neutralization: new insights into the problem of employee information systems security policy violations," MIS Quarterly. 34(3), 2010, pp. 487-502.
[19] B. Lu, X. Guo, N. Luo, and G. Chen, "Corporate blogging and job performance: effects of work-related and non-work-related participation," Journal of Management Information Systems, 32(4), 2015, pp. 285-314.
[20] K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding nonmalicious security violations in the workplace: a composite behavior model," Journal of Management Information Systems, 28(2), 2011, pp. 203-236.
[21] G. D. Moody and M. Siponen, "Using the theory of interpersonal behavior to explain non-work-related personal use of the internet at work," Information & Management, 50(6), 2013, pp. 322-335.
[22] A. L. Blanchard and C. A. Henle, "Correlates of different forms of cyberloafing: the role of norms and external locus of control," Computers in Human Behavior, 24(3), 2008, pp. 1067-1084.
[23] A. Vance, P. B. Lowry and D. Eggett, "Using accountability to reduce access policy violations in information systems," Journal of Management Information Systems, 29(4), 2013, pp. 263-290.
[24] H. Jia, R. Jia and S. Karau, "Cyberloafing and personality: the impact of the big five traits and workplace situational factors," Journal of Leadership & Organizational Studies, 20(3), 2013, pp. 358-365.
[25] K. Kim, M. del Carmen Triana, K. Chung, and N. Oh, "When do employees cyberloaf? An interactionist perspective examining personality, justice, and empowerment," Human Resource Management, 55(6), 2016, pp. 1041-1058.
[26] L. Khansa, J. Kuem, M. Siponen and S. S. Kim, "To cyberloaf or not to cyberloaf: the impact of the announcement of formal organizational controls," Journal of Management Information Systems, 34(1), 2017, pp. 141-176.
[27] I. Vranjes, E. Baillien, H. Vandebosch, S. Erreygers, and H. De Witte, "The dark side of working online: towards a definition and an emotion reaction model of workplace cyberbullying," Computers in Human Behavior, 69, 2017, pp. 324-334.
[28] A. Nocentini, J. Calmaestra, A. Schultze-Krumbholz, H. Scheithauer, R. Ortega, and E. Menesini, "Cyberbullying: labels, behaviours and definition in three european countries," Australian Journal of Guidance & Counselling, 20(2), 2010, pp. 129-142.
[29] M. Taylor, J. Haggerty, D. Gresty, N. Criado Pacheco, T. Berry, and P. Almond, "Investigating employee harassment via social media," Journal of Systems and Information Technology, 17(4), 2015, pp. 322-335.
[30] S. L. Robinson and E. W. Morrison, "The development of psychological contract breach and violation: a longitudinal study," Journal of Organizational Behavior, 21(5), 2000, pp. 525-546.
[31] S. L. Robinson, "Trust and breach of the psychological contract," Administrative Science Quarterly, 41, 1996, pp. 574-599.
[32] E. Ahmed and M. Muchiri, "Linking abusive supervision to employees' OCBs and turnover intentions: the role of a psychological contract breach and perceived organizational support," Contemporary Management Research, 10(2), 2014, pp. 147-164.
[33] S. F. Chiu and J. C. Peng, "The relationship between psychological contract breach and employee deviance: the moderating role of hostile attributional style," Journal of Vocational Behavior, 73(3), 2008, pp. 426-433.
[34] J. C. Peng, J. J. Jien and J. Lin, "Antecedents and consequences of psychological contract breach," Journal of Managerial Psychology, 31(8), 2016, pp. 1312-1326.
[35] J. Han, Y. J. Kim and H. Kim, "An integrative model of information security policy compliance with

psychological contract: examining a bilateral perspective," Computers & Security, 66, 2017, pp. 52-65.
[36] T. C. Lin, S. L. Huang and S. C. Chiang, "User resistance to the implementation of information systems: a psychological contract breach perspective," Journal of the Association for Information Systems, 19(4), 2018, pp. 306-332.
[37] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," MIS Quarterly, 34(3), 2010, pp.393 523-548.
[38] B. W. Guan and C. Hsu. "The role of abusive supervision and organizational commitment on employees' information security policy noncompliance intention," Internet Research, 30(5), 2020, pp. 1383-1405.
[39] W. He, "A review of social media security risks and mitigation techniques," Journal of Systems and Information Technology, 14(2), 2012, pp. 171-180.
[40] L. Thornthwaite, "Chilling times: social media policies, labor law and employment relations," Asia Pacific Journal of Human Resources, 54(3), 2016, pp. 332-351.
[41] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness," Decision Support Systems, 47(2), 2009, pp. 154-165.
[42] P. B. Lowry, C. Posey, R. J. Bennett, and T. L. Roberts, "Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust," Information Systems Journal, 25(3), 2015, pp. 193-273.
[43] J. C. Ugrin, J. M. Pearson, and M. D. Odom, "Cyberslacking: self-control, prior behavior and the impact of deterrence measures," Review of Business Information Systems, 12(1), 2008, pp. 75-88.
[44] C. A. Henle and A. L. Blanchard. "The interaction of work stressors and organizational sanctions on cyberloafing," Journal of Managerial Issues, 20, 2008, pp. 383–400.
[45] R. Paternoster and S. Simpson, "Sanction threats and appeals to morality: testing a rational choice model of corporate crime," Law & Society Review, 30(3), 1996, pp. 549-584.
[46] A. Piquero ad S. Tibbetts, "Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: toward a more complete model of rational offending," Justice Quarterly, 13(3), 1996, pp. 481-510.
[47] R. C. Hollinger, J. P. Clark. "Formal and informal social controls of employee deviance," The Sociological Quarterly, 23(3), 1982, pp. 333-343.
[48] A. C. Johnston, M. Warkentin and M. Siponen, "An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric," MIS Quarterly, 39(1), 2015, pp. 113-134.
[49] P. B. Lowry, J. Zhang, C. Wang and M. Siponen, "Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning (SSSL) model," Information Systems Research, 27, 2016, pp. 962-986.
[50] J. C. Nunnally, "Psychometric theory," 2nd (Ed.), McGraw-Hill, New York, 1978.
[51] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," Journal of Marketing Research, 18(1), 1981, pp. 39-50.
[52] H. W. Marsh, Z. Wen, and K. T. Han, "Structural equation models of latent interactions: evaluation of alternative estimation strategies and indicator construction," Psychological Methods, 9(3), 2004, pp. 275-300.
[53] G. C. Lin, Z. Wen, H. W. Marsh, and H. S. Lin, "Structural equation models of latent interactions: clarification of orthogonalizing and double-mean-centering strategies," Structural Equation Modeling: A Multidisciplinary Journal, 17(3), 2010, pp. 374-391.
[54] D. P. MacKinnon, C. M. Lockwood, J. M. Hoffman, S. G. West, & V. Sheets, "A comparison of methods to test mediation and other intervening variable effects," Psychological methods, *7*(1), 2002, pp. 83–104.
[55] X. Zhao, J. G. Lynch, Q. Chen, "Reconsidering Baron and Kenny: Myths and truths about mediation analysis." Journal of Consumer Research, 37(2), 2010, pp. 197–206.
[56] J. F. Dawson, "Moderation in management research: what, why, when and how," Journal of Business and Psychology, 29(1), 2014, pp. 1-19.
[57] R. J. Bies, and J. F. Moag, "Interactional justice: communication criteria of fairness," In R. J. Lewicki, B. H. Sheppard, M. H. Bazerman (Eds.), Research on Negotiations in Organizations, 1, JAI Press, Greenwich, 1986, pp. 43-55.